EXAM CRAM

The Smart Way to Study™

Exam SY0-201

CompTIA® Security+

Second Edition

Diane Barrett
Kirk Hausman
Martin Weiss

CompTIA Security+ Exam Cram, Second Edition

ISBN-13: 978-0-7897-3804-2
ISBN-10: 0-7897-3804-x

Library of Congress Cataloging-in-Publication Data

Barrett, Diane.

CompTIA security+ exam cram / Diane Barrett, Kalani K. Hausman, and Martin Weiss. — 2nd ed.

p. cm.

ISBN 978-0-7897-3804-2 (pbk. w/cd)

1. Electronic data processing personnel—Certification. 2. Computer networks—Examinations—Study guides. 3. Computer technicians—Certification—Study guides. I. Hausman, Kalani Kirk. II. Weiss, Martin. III. Title.

QA76.3.B3644 2009

004.6—dc22

2008045337

Printed in the United States on America

First Printing: November 2008

Trademarks

Warning and Disclaimer

Bulk Sales

Que Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales

1-800-382-3419

corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales

international@pearsoned.com

Associate Publisher
David Dusthimer

Executive Editor
Betsy Brown

Development Editor
Dayna Isley

Technical Editors
Pawan Bhardwaj

Christopher Crayton

Managing Editor
Patrick Kanouse

Project Editor
Seth Kerney

Copy Editor
Keith Cline

Indexer
Joy Dean Lee

Proofreader
Language Logistics, LLC

Publishing Coordinator
Vanessa Evans

Book Designer
Gary Adair

Page Layout
Bronkella Publishing

Introduction

Welcome to *CompTIA Security+ Exam Cram*, Second Edition. Whether this book is your first or your fifteenth *Exam Cram* series book, you'll find information here that will help ensure your success as you pursue knowledge, experience, and certification. This book aims to help you get ready to take and pass the CompTIA Security+ exam, number SY0-201.

This introduction explains CompTIA's certification programs in general and talks about how the *Exam Cram* series can help you prepare for CompTIA's latest certification exams. Chapters 1 through 12 are designed to remind you of everything you need to know to pass the SY0-201 certification exam. The two practice exams at the end of this book should give you a reasonably accurate assessment of your knowledge; and, yes, we've provided the answers and their explanations for these practice exams. Read this book, understand the material, and you'll stand a very good chance of passing the real test.

Exam Cram books help you understand and appreciate the subjects and materials you need to know to pass CompTIA certification exams. *Exam Cram* books are aimed strictly at test preparation and review. They do not teach you everything you need to know about a subject. Instead, the authors streamline and highlight the pertinent information by presenting and dissecting the questions and problems they've discovered that you're likely to encounter on a CompTIA test.

Nevertheless, to completely prepare yourself for any CompTIA test, we recommend that you begin by taking the "Self-Assessment" that immediately follows this introduction. The self-assessment tool will help you evaluate your knowledge base against the requirements for the CompTIA Security+ exam under both ideal and real circumstances. This can also be the first step in earning more advanced security certifications.

Based on what you learn from the self-assessment, you might decide to begin your studies with classroom training or some background reading. On the other hand, you might decide to pick up and read one of the many study guides available from Que or a third-party vendor.

We also strongly recommend that you spend some time installing, configuring, and working with both Windows and UNIX or Linux operating systems to patch and maintain them for the best and most current security possible because the Security+ exam focuses on such activities and the knowledge and skills they can provide for you. Nothing beats hands-on experience and familiarity when it

comes to understanding the questions you're likely to encounter on a certification test. Book learning is essential, but without doubt, hands-on experience is the best teacher of all!

The CompTIA Certification Program

The Computing Technology Industry Association (http://www.comptia.org) offers numerous IT certifications, primarily aimed at entry- and intermediate-level IT professionals. Here is a list of some other relevant CompTIA certifications, briefly annotated to document their possible relevance to Security+:

- *A+*: An exam that tests basic PC hardware and software installation, configuration, diagnosing, preventive maintenance, and basic networking. This two-part exam also covers security, safety, environmental issues, communication, and professionalism. This exam is an excellent prequalifier for those interested in Security+ who might have little or no PC or computing skills or knowledge. For more information about this exam, see http://certification.comptia.org/a/default.aspx.
- *Network+*: An exam that tests basic and intermediate networking skills and knowledge, including hardware, drivers, protocols, and troubleshooting topics. This exam is an excellent prequalifier for those interested in Security+ who have little or no networking skills or knowledge. For more information about this exam, go to http://certification.comptia.org/network/default.aspx.
- *Server+*: An exam that tests server knowledge and capabilities, including RAID, SCSI, multiple CPUs, and disaster recovery. This exam is an excellent prequalifier for those interested in Security+ who have little or no server environment skills or knowledge. For more information about this exam, go to http://certification.comptia.org/server/default.aspx.
- *Linux+*: An exam that tests knowledge and management of Linux systems via command line, user administration, file permissions, software configurations, Linux-based clients, server systems, and security. For more information about this exam, go to http://certification.comptia.org/linux/default.aspx.

The CompTIA exams are all vendor- and platform-neutral, which means they primarily test general skills and knowledge, instead of focusing on vendor or product specifics. Therefore, they offer certification candidates a chance to

demonstrate necessary general abilities relevant in most workplaces. (This explains why employers generally look at CompTIA certifications favorably.)

Because CompTIA changes their website often, the URLs listed above might not work in the future. You should use the Search tool on CompTIA's site to find more information about a particular certification.

Taking a Certification Exam

After you prepare for your exam, you need to register with a testing center. At the time of this writing, the cost to take the Security+ exam is $258 for individuals. CompTIA Corporate Members receive discounts on nonmember pricing. For more information about these discounts, a local CompTIA sales representative can provide answers to any questions you might have. If you don't pass, you can take the exam again for the same cost as the first attempt, for each attempt until you pass. In the United States and Canada, tests are administered by Prometric or VUE. Here's how you can contact them:

- *Prometric*—You can sign up for a test through the company's website, http://securereg3.prometric.com/. Within the United States and Canada, you can register by phone at 800-755-3926. If you live outside this region, check the Prometric website for the appropriate phone number.
- *Pearson VUE*—You can contact Virtual University Enterprises (VUE) to locate a nearby testing center that administers the test and to make an appointment. You can find the sign-up web page for the exam itself at http://www.vue.com/comptia/. You can also use this web page (click the Contact button, click the View Telephone Directory by Sponsor link, and then click CompTIA) to obtain a telephone number for the company (in case you can't or don't want to sign up for the exam on the web page).

To sign up for a test, you must possess a valid credit card or contact either Prometric or Vue for mailing instructions to send a check (in the United States). Only after payment has been verified, or a check has cleared, can you actually register for a test.

To schedule an exam, you need to call the appropriate phone number or visit the Prometric or Vue website at least one day in advance. To cancel or reschedule an exam in the United States or Canada, you must call before 3 p.m. Eastern time the day before the scheduled test time (or you might be charged, even if you don't show up to take the test). When you want to schedule a test, you should have the following information ready:

- Your name, organization, and mailing address.
- Your CompTIA test ID. (In the United States, this means your Social Security number; citizens of other countries should call ahead to find out what type of identification number is required to register for a test.)
- The name and number of the exam you want to take.
- A payment method. (As mentioned previously, a credit card is the most convenient method; alternative means can be arranged in advance, if necessary.)

After you sign up for a test, you are told when and where the test is scheduled. You should arrive at least 15 minutes early. To be admitted into the testing room, you must supply two forms of identification, one of which must be a photo ID.

Tracking Certification Status

After you pass the exam, you are certified. Official certification is normally granted after six to eight weeks, so you shouldn't expect to get your credentials overnight. The package for official certification that arrives includes a Welcome Kit that contains a number of elements. (See CompTIA's website for other benefits of specific certifications.)

- A certificate suitable for framing, along with a wallet card.
- A license to use the related certification logo, which means you can use the logo in advertisements, promotions, and documents, and on letterhead, business cards, and so on. Along with the license comes a logo sheet, which includes camera-ready artwork. (Note that before you use any of the artwork, you must sign and return a licensing agreement that indicates you'll abide by its terms and conditions.)

Many people believe that the benefits of certification go well beyond the perks that CompTIA provides to new members of this elite group. We're starting to see more job listings that request or require applicants to have CompTIA and other related certifications, and many individuals who complete CompTIA certification programs can qualify for increases in pay and responsibility. As an official recognition of hard work and broad knowledge, a certification credential is a badge of honor in many IT organizations.

About This Book

We've structured the topics in this book to build on one another. Therefore, some topics in later chapters make the most sense after you've read earlier chapters. That's why we suggest that you read this book from front to back for your initial test preparation. If you need to brush up on a topic or if you have to bone up for a second try, you can use the index or table of contents to go straight to the topics and questions that you need to study. Beyond helping you prepare for the test, we think you'll find this book useful as a tightly focused reference to some of the most important aspects of the Security+ certification.

Chapter Format and Conventions

Each topical *Exam Cram* chapter follows a regular structure and contains graphical cues about important or useful information. Here's the structure of a typical chapter:

- *Opening hotlists*—Each chapter begins with a list of the terms, tools, and techniques that you must learn and understand before you can be fully conversant with that chapter's subject matter. The hotlists are followed with one or two introductory paragraphs to set the stage for the rest of the chapter.
- *Topical coverage*—After the opening hotlists and introductory text, each chapter covers a series of topics related to the chapter's subject. Throughout that section, we highlight topics or concepts that are likely to appear on a test, using a special element called an Exam Alert:

EXAM ALERT

This is what an alert looks like. Normally, an alert stresses concepts, terms, software, or activities that are likely to relate to one or more certification test questions. For that reason, we think any information in an alert is worthy of extra attentiveness on your part.

Pay close attention to material flagged in Exam Alerts; although all the information in this book pertains to what you need to know to pass the exam, Exam Alerts contain information that is *really* important. Of course, you need to understand the "meat" of each chapter, too, when

preparing for the test. Because this book's material is condensed, we recommend that you use this book along with other resources to achieve the maximum benefit.

In addition to the alerts, we provide tips and notes to help you build a better foundation for security knowledge. Although the tip information might not be on the exam, it is certainly related and will help you become a better-informed test taker.

TIP

This is how tips are formatted. Keep your eyes open for these, and you'll become a Security+ guru in no time!

NOTE

This is how notes are formatted. Notes direct your attention to important pieces of information that relate to the CompTIA Security+ certification.

- *Exam prep questions*—Although we talk about test questions and topics throughout this book, the section at the end of each chapter presents a series of mock test questions and explanations of both correct and incorrect answers.
- *Details and resources*—Every chapter ends with a section that provides direct pointers to CompTIA and third-party resources that offer more information about the chapter's subject. That section also tries to rank or at least rate the quality and thoroughness of the topic's coverage by each resource. If you find a resource you like in that collection, you should use it; don't feel compelled to use all the resources. On the other hand, we recommend only resources that we use on a regular basis, so none of our recommendations will be a waste of your time or money. (However, purchasing them all at once probably represents an expense that many network administrators and CompTIA certification candidates might find hard to justify.)

Although the bulk of this book follows this chapter structure just described, we want to point out a few other elements:

- "Practice Exam 1" and "Practice Exam 2" and the answer explanations provide good reviews of the material presented throughout the book to ensure that you're ready for the exam.
- The Glossary defines important terms used in this book.
- The tear-out Cram Sheet attached next to the inside front cover of this book represents a condensed collection of facts and tips that we think are essential for you to memorize before taking the test. Because you can dump this information out of your head onto a sheet of paper just before taking the exam, you can master this information by brute force; you need to remember it only long enough to write it down when you walk into the testing room. You might even want to look at it in the car or in the lobby of the testing center just before you walk in to take the exam.
- The MeasureUp Practice Tests CD-ROM that comes with each *Exam Cram* and *Exam Prep* book features a powerful, state-of-the-art test engine that prepares you for the actual exam. MeasureUp Practice Tests are developed by certified IT professionals and are trusted by certification students around the world. For more information, visit http://www.measureup.com.

Exam Topics

Table I-1 lists the skills measured by the SY0-201 exam and the chapter in which the topic is discussed. Some topics are covered in other chapters, too.

TABLE I-1 CompTIA SY0-201 Exam Topics

Exam Topic	Chapter
Domain 1.0: Systems Security	
Differentiate among various systems security threats.	1
Explain the security risks pertaining to system hardware and peripherals.	1
Implement OS hardening practices and procedures to achieve workstation and server security.	7
Carry out the appropriate procedures to establish application security.	2
Implement security applications.	4
Explain the purpose and application of virtualization technology.	4
Domain 2.0: Network Infrastructure	
Differentiate between the different ports and protocols and their respective threats and mitigation techniques.	3
Distinguish between network design elements and components.	3
Determine the appropriate use of network security tools to facilitate network security.	3
Apply the appropriate network tools to facilitate network security.	4
Evaluate user systems and recommend appropriate settings to optimize performance.	4
Explain the vulnerabilities and mitigations associated with network devices.	2
Explain the vulnerabilities and mitigations associated with various transmission media.	2
Explain the vulnerabilities and implement mitigations associated with wireless networking.	6
Domain 3.0: Access Control	
Identify and apply industry best practices for access control methods.	5
Explain common access control models and the differences between each.	5
Organize users and computers into appropriate security groups and roles while distinguishing between appropriate rights and privileges.	4
Apply appropriate security controls to file and print resources.	4
Compare and implement logical access control methods.	4
Summarize the various authentication models and identify the components of each.	5
Deploy various authentication models and identify the components of each.	6
Explain the difference between identification and authentication (identity proofing).	5
Explain and apply physical access security methods.	5
Domain 4.0: Assessments and Audits	
Conduct risk assessments and implement risk mitigation.	7
Carry out vulnerability assessments using common tools.	7
Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning.	7

TABLE I-1 *Continued*

Exam Topic	Chapter
Domain 4.0: Assessments and Audits	
Use monitoring tools on systems and networks and detect security-related anomalies.	8
Compare and contrast various types of monitoring methodologies.	8
Execute proper logging procedures and evaluate the results.	8
Conduct periodic audits of system security settings.	8
Domain 5.0: Cryptography	
Explain general cryptography concepts.	9
Explain basic hashing concepts and map various algorithms to appropriate applications.	9
Explain basic encryption concepts and map various algorithms to appropriate applications.	9
Explain and implement protocols.	10
Explain core concepts of public key cryptography.	10
Implement PKI and certificate management.	10
Domain 6.0: Organizational Security	
Explain redundancy planning and its components.	11
Implement disaster recovery procedures.	11
Differentiate between and execute appropriate incident response procedures.	12
Identify and explain applicable legislation and organizational policies.	12
Explain the importance of environmental controls.	12
Explain the concept of and how to reduce the risks of social engineering.	12

Given all the book's elements and its specialized focus, we've tried to create a tool that will help you prepare for and pass CompTIA Security+ Exam SY0-201. Please share with us your feedback on this book, especially if you have ideas about how we can improve it for future test takers. Send your questions or comments about this book via email to feedback@quepublishing.com. We'll consider everything you say carefully, and we'll respond to all suggestions. For more information about this book and other *Exam Cram* titles, visit our website at http://www.informit.com/examcram.

Thanks for making this *Exam Cram* book a pivotal part of your certification study plan. Best of luck on becoming certified!

3

CHAPTER THREE

Infrastructure Basics

Terms you need to understand:

- ✓ TCP/IP hijacking
- ✓ Spoofing
- ✓ Man-in-the-middle
- ✓ Replay
- ✓ DoS
- ✓ DNS kiting and DNS poisoning
- ✓ ARP poisoning
- ✓ DMZ
- ✓ VLAN
- ✓ NAT
- ✓ NAC
- ✓ NIDS
- ✓ HIDS
- ✓ NIPS
- ✓ Protocol analyzers

Techniques you need to master:

- ✓ Differentiate between the different ports and protocols, their respective threats, and mitigation techniques.
- ✓ Distinguish between network design elements and components.
- ✓ Determine the appropriate use of network security tools to facilitate network security.
- ✓ Apply the appropriate network tools to facilitate network security.
- ✓ Explain the strengths and vulnerabilities of various security zones and devices.

The network infrastructure is subject to myriad internal and external attacks through services, protocols, and open ports. It is imperative that you understand how to eliminate nonessential services and protocols, especially if the network has been in existence for some period of time and some services are no longer needed or have been forgotten. To stop many would-be attackers, you must understand the different types of attacks that can happen, along with how to implement a network design, components, and tools that can protect the infrastructure.

This chapter discusses the concepts of identifying and mitigating network infrastructure threats and alerts you to the most common attacks. In addition to being able to explain these concepts, you will begin to understand how network design and components can be used as a tool to protect and mitigate all types of threats and to protect computers and network infrastructure.

Port and Protocol Threats and Mitigation Techniques

There are 65,535 TCP and UDP ports on which a computer can communicate. The port numbers are divided into three ranges:

- *Well-known ports*—The well-known ports are those from 0 through 1,023.
- *Registered ports*—The registered ports are those from 1,024 through 49,151.
- *Dynamic/private ports*—The dynamic/private ports are those from 49,152 through 65,535.

Often, many of these ports are not secured and as a result are used for exploitation. Table 3.1 lists some of the most commonly used ports and the services and protocols that use them. All of these ports and services have vulnerabilities associated with them. Some of these were discussed in Chapter 2, "Online Vulnerabilities," and some are discussed in this chapter. For those that are not discussed, such as Echo, Systat, and Chargen, you can find more detailed information in the "Suggested Reading and Resources" section at the end of this chapter.

EXAM ALERT

Know the difference between the various types of attacks and the ports they are executed on.

TABLE 3.1 Commonly Used Ports

Port	Service/Protocol
7	Echo
11	Systat
15	Netstat
19	Chargen
20	FTP-Data
21	FTP
22	SSH
23	Telnet
25	SMTP
49	TACACS
53	DNS
80	HTTP
110	POP3
111	Portmap
137, 138, 139	NetBIOS
161/162	SNMP
443	HTTPS
445	SMB
1,812	RADIUS

Ideally, the configuration process should start with installing only the services necessary for the server to function. Table 3.1 includes a combination of protocols that currently are in use and antiquated protocols that might still be in use on a network. These protocols may be configured open by default when an operating system is installed or by the machine manufacturer. Every operating system requires different services for it to operate properly. If ports are opened for manufacturer-installed tools, the manufacturer should have these services listed in the documentation. The next sections cover port and protocol threats and mitigation techniques.

Antiquated and Older Protocols

Notice in Table 3.1 that there are older protocols such as Chargen and Telnet. Although these may be older, you might find that these protocols and the ports they use are still accessible. For example, Finger, which uses port 79, was widely used during the early days of Internet, and today's sites no longer offer the service. However, you might still find some old implementations of Eudora mail that use the Finger protocol, or worse, the mail clients have long since been upgraded, but the port used 10 years ago was somehow left open. The quickest way to tell which ports are open and which services are running is to do a Netstat on the machine. You can also run local or online port scans.

Older protocols that are still in use may leave the network vulnerable. Protocols such as Simple Network Management Protocol (SNMP) and domain name service (DNS) that were developed a long time ago and have been widely deployed can pose security risks, too. SNMP is an application layer protocol whose purpose is to collect statistics from TCP/IP devices. SNMP is used for monitoring the health of network equipment, computer equipment, and devices such as uninterruptible power supplies (UPSs). Many of the vulnerabilities associated with SNMP stem from using SNMPv1. Although these vulnerabilities were discovered in 2002, vulnerabilities are still being reported with current SNMP components. A recent Gentoo Linux Security Advisory noted that multiple vulnerabilities in Net-SNMP allow for authentication bypass and execution of arbitrary code in Perl applications using Net-SNMP.

The SNMP management infrastructure consists of three components:

- SNMP managed node
- SNMP agent
- SNMP network management station

The device loads the agent, which in turn collects the information and forwards it to the management station. Network management stations collect a massive amount of critical network information and are likely targets of intruders because SNMPv1 is not secure. The only security measure it has in place is its community name, which is similar to a password. By default, this is "public" and many times is not changed, thus leaving the information wide open to intruders. SNMPv2 uses Message Digest Version 5 (MD5) for authentication. The transmissions can also be encrypted. SNMPv3 is the current standard, but some devices are likely to still be using SNMPv1 or SNMPv2.

SNMP can help malicious users learn a lot about your system, making password guessing attacks a bit easier. SNMP is often overlooked when checking for vulnerabilities because it uses User Datagram Protocol (UDP) ports 161 and 162. Make sure network management stations are secure physically and secure on the network. You might even consider using a separate management subnet and protecting it using a router with an access list. Unless this service is required, it should be turned off.

The best way to protect the network infrastructure from attacks aimed at antiquated or unused ports and protocols is to remove any unnecessary protocols and create access control lists to allow traffic on necessary ports only. By doing so, you eliminate the possibility of unused and antiquated protocols being exploited and minimize the threat of an attack.

TCP/IP Hijacking

Hijacking is the term used when an attacker takes control of a session between the server and a client. This starts as a man-in-the-middle attack and then adds a reset request to the client. The result is that the client gets kicked off the session, while the rogue machine still communicates with the server. The attacker intercepts the source-side packets and replaces them with new packets that are sent to the destination.

EXAM ALERT

TCP/IP hijacking commonly happens during Telnet and web sessions where security is lacking or when session timeouts aren't configured properly.

During web sessions, cookies are commonly used to authenticate and track users. While the authenticated connection is in session, an attacker may be able to hijack the session by loading a modified cookie in the session page. Session hijacking can also occur when a session timeout is programmed to be a long period of time. This provides a chance for an attacker to hijack the session.

Telnet type plain-text connections create the ideal situation for TCP hijacking. In this instance, an attacker watches the data being passed in the TCP session. At any point, the attacker can take control of the user's session. This is why TCP/IP hijacking is also called *session hijacking*.

Forcing a user to reauthenticate before allowing transactions to occur could help prevent this type of attack. Protection mechanisms include the use of unique initial sequence numbers (ISNs) and web session cookies. The more unique the

cookie, the harder it is to break and hijack. Additional preventative measures for this type of attack include use of encrypted session keys and Secure Sockets Layer (SSL) encryption.

Null Sessions

A *null session* is a connection without specifying a username or password. Null sessions are a possible security risk because the connection is not really authenticated. A program or service using the system user account logs on with null credentials, and in some web-based programs, the set of credentials used for authentication defaults to anonymous access when null credentials are given. A hacker or worm can exploit this vulnerability and potentially access sensitive data on the system.

The best example of this is file and print sharing services on Windows machines. The services communicate by using an interprocess communication share, or IPC$. You have likely seen this on Windows machines (see Figure 3.1).

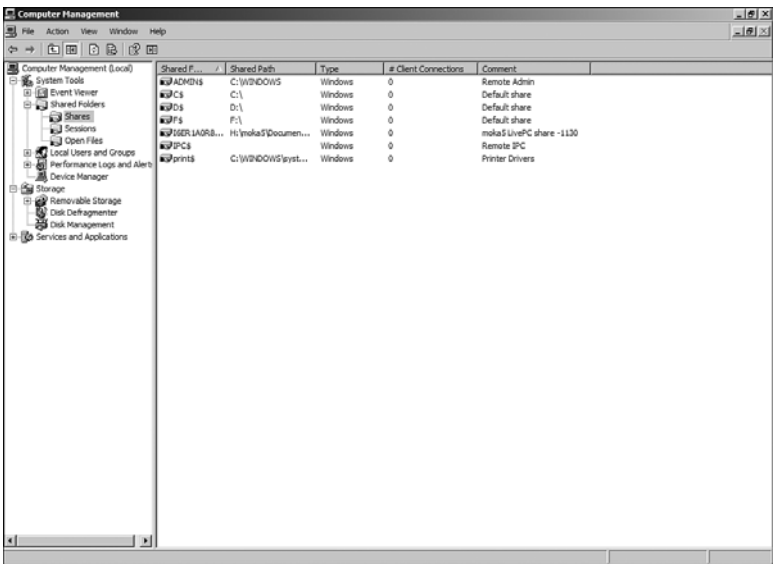

FIGURE 3.1 A Windows IPC$ share.

These null sessions were created to allow unauthenticated hosts to obtain browse lists from Windows NT servers and to use network file and print sharing services. By default, Windows XP and Windows Server 2003 standalone servers are not vulnerable to null session attacks. However, backward compatibility with Windows 2000 and NT open up vulnerability to null session attacks.

On a vulnerable machine, even if you have disabled the Guest account, a null session can be established by using the `net use` command to map a connection using a blank username and password:

```
net use \\ip_address\ipc$ "" "/user:"
```

After a null session connection has been established, many possibilities exist. You can use commands such as `net view` to view a list of shared resources on the target machine. You also can use application programming interfaces (APIs) and remote procedure calls (RPCs) to enumerate information, escalate privileges, and execute attacks.

EXAM ALERT

The most effective way to reduce null session vulnerability is by disabling NetBIOS over TCP/IP. After you have this, verify that ports 139 and 445 are closed.

You could also control null session access by editing the Registry on Windows-based computers to restrict anonymous access:

- *Key*—HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA
- *Value*—RestrictAnonymous
- *Type*—DWORD
- *Value*—1

The key default value is 0. Changing this value to 1, which is more restrictive, keeps a null session from seeing user accounts and admin shares. Changing the value to 2 is the most restrictive. This disables null session without explicit permissions. However, this setting may conflict with some applications that rely on null sessions. Keep in mind that even though you can change the Registry settings to try to prevent this type of attack, some tools sidestep this measure. If security is a major concern, you might have to consider not allowing any null sessions on your public and private networks.

Spoofing

Spoofing is a method of providing false identity information to gain unauthorized access. This is accomplished by modifying the source address of traffic or source of information.

EXAM ALERT

Spoofing seeks to bypass IP address filters by setting up a connection from a client and sourcing the packets with an IP address that is allowed through the filter.

In *blind spoofing*, the attacker sends only data and only makes assumptions of responses. In *informed spoofing*, the attacker can participate in a session and can monitor the bidirectional communications.

Services such as email, Web, and file transfer can also be spoofed. Web spoofing happens when an attacker creates a convincing but false copy of an entire website. The false site looks just like the real one: It has all the same pages and links. However, the attacker controls the false site so that all network traffic between the victim's browser and the site goes through the attacker. In email spoofing, a spammer or a computer virus can forge the email packet information in an email so that it appears the email is coming from a trusted host, from one of your friends, or even from your own email address. If you leave your email address at some Internet site or exchange email with other people, a spoofer may be able to use your email address as the sender address to send spam. File-transfer spoofing involves the FTP service. FTP data is sent in clear text. The data can be intercepted by an attacker. The data could then be viewed and altered before sending it on to the receiver. These forms of attacks are often used to get additional information from network users to complete a more aggressive attack.

You should set up a filter that denies traffic originating from the Internet that shows an internal network address. Using the signing capabilities of certificates on servers and clients allows web and email services to be more secure. The use of IPsec can secure transmissions between critical servers and clients. This will help prevent these types of attacks from taking place.

Man in the Middle

The *man-in-the-middle attack* takes place when an attacker intercepts traffic and then tricks the parties at both ends into believing that they are communicating with each other. This type of attack is possible because of the nature of the three-way TCP handshake process using SYN and ACK packets. Because TCP is a connection-oriented protocol, a three-way handshake takes place when establishing a connection and when closing a session. When establishing a session, the client sends a SYN request, then the server sends an acknowledgment and synchronization (SYN-ACK) to the client, and then the client sends an ACK (also referred to as SYN-ACK-ACK), completing the connection. During this process, the attacker initiates the man-in-the-middle attack. The attacker

uses a program that appears to be the server to the client and appears to be the client to the server. The attacker can also choose to alter the data or merely eavesdrop and pass it along. This attack is common in Telnet and wireless technologies. It is also generally difficult to implement because of physical routing issues, TCP sequence numbers, and speed. Because the hacker has to be able to sniff both sides of the connection simultaneously, programs such as Juggernaut, T-Sight, and Hunt have been developed to help make the man-in-the-middle attack easier.

If the attack is attempted on an internal network, physical access to the network will be required. Be sure that access to wiring closets and switches is restricted; if possible, the area should be locked.

After you have secured the physical environment, the services and resources that allow a system to be inserted into a session should be protected. DNS can be compromised and used to redirect the initial request for service, providing an opportunity to execute a man-in-the-middle attack. DNS access should be restricted to read-only for everyone except the administrator. The best way to prevent these types of attacks is to use encryption and secure protocols.

EXAM ALERT

A man-in-the-middle attack takes place when a computer intercepts traffic and either eavesdrops on the traffic or alters it.

Replay

In a *replay attack*, packets are captured by using sniffers. After the pertinent information is extracted, the packets are placed back on the network. This type of attack can be used to replay bank transactions or other similar types of data transfer in the hopes of replicating or changing activities, such as deposits or transfers.

Protecting yourself against replay attacks involves some type of time stamp associated with the packets or time-valued, nonrepeating serial numbers. Secure protocols such as IPsec prevent replays of data traffic in addition to providing authentication and data encryption.

Denial of Service

The purpose of a denial-of-service (DoS) attack is to disrupt the resources or services that a user would expect to have access to. These types of attacks are

executed by manipulating protocols and can happen without the need to be validated by the network. An attack typically involves flooding a listening port on your machine with packets. The premise is to make your system so busy processing the new connections that it cannot process legitimate service requests.

Many of the tools used to produce DoS attacks are readily available on the Internet. Administrators use them to test connectivity and troubleshoot problems on the network, whereas malicious users use them to cause connectivity issues.

Here are some examples of DoS attacks:

- *Smurf/smurfing*—This attack is based on the Internet Control Message Protocol (ICMP) echo reply function. It is more commonly known as *ping*, which is the command-line tool used to invoke this function. In this attack, the attacker sends ping packets to the broadcast address of the network, replacing the original source address in the ping packets with the source address of the victim, thus causing a flood of traffic to be sent to the unsuspecting network device.
- *Fraggle*—This attack is similar to a Smurf attack. The difference is that it uses UDP rather than ICMP. The attacker sends spoofed UDP packets to broadcast addresses as in the Smurf attack. These UDP packets are directed to port 7 (Echo) or port 19 (Chargen). When connected to port 19, a character generator attack can be run. Table 3.1 lists the most commonly exploited ports.
- *Ping flood*—This attack attempts to block service or reduce activity on a host by sending ping requests directly to the victim. A variation of this type of attack is the ping of death, in which the packet size is too large and the system doesn't know how to handle the packets.
- *SYN flood*—This attack takes advantage of the TCP three-way handshake. The source system sends a flood of synchronization (SYN) requests and never sends the final acknowledgment (ACK), thus creating half-open TCP sessions. Because the TCP stack waits before resetting the port, the attack overflows the destination computer's connection buffer, making it impossible to service connection requests from valid users.
- *Land*—This attack exploits a behavior in the operating systems of several versions of Windows, UNIX, Macintosh OS, and Cisco IOS with respect to their TCP/IP stacks. The attacker spoofs a TCP/IP SYN packet to the victim system with the same source and destination IP address and

the same source and destination ports. This confuses the system as it tries to respond to the packet.

- *Teardrop*—This form of attack targets a known behavior of UDP in the TCP/IP stack of some operating systems. The Teardrop attack sends fragmented UDP packets to the victim with odd offset values in subsequent packets. When the operating system attempts to rebuild the original packets from the fragments, the fragments overwrite each other, causing confusion. Because some operating systems cannot gracefully handle the error, the system will most likely crash or reboot.
- *Bonk*—This attack affects mostly Windows 95 and NT machines by sending corrupt UDP packets to DNS port 53.The attack modifies the fragment offset in the packet. The target machine then attempts to reassemble the packet. Because of the offset modification, the packet is too big to be reassembled, and the system crashes.
- *Boink*—This is a Bonk attack that targets multiple ports rather than just port 53.

DoS attacks come in many shapes and sizes. The first step to protecting yourself from an attack is to understand the nature of different types of attacks in the preceding list.

Distributed DoS

Another form of attack is a simple expansion of a DoS attack, referred to as a *distributed DoS (DDoS) attack*. Masters are computers that run the client software, and zombies run software. The attacker creates masters, which in turn create a large number of zombies or recruits. The software running on the zombies can launch multiple types of attacks, such as UDP or SYN floods on a particular target. A typical DDoS is shown in Figure 3.2.

In simple terms, the attacker distributes zombie software that allows the attacker partial or full control of the infected computer system.

EXAM ALERT

When an attacker has enough systems compromised with the installed zombie software, he can initiate an attack against a victim from a wide variety of hosts. The attacks come in the form of the standard DoS attacks, but the effects are multiplied by the total number of zombie machines under the control of the attacker.

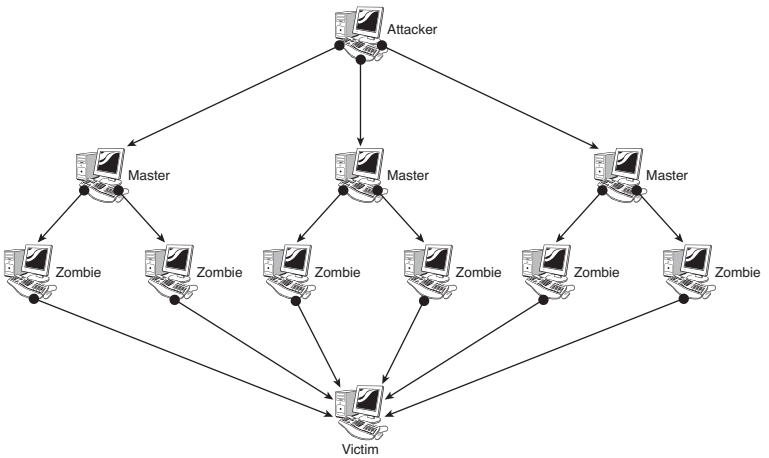

FIGURE 3.2 A DDoS attack.

Although DDoS attacks generally come from outside the network to deny services, the impact of DDoS attacks mounted from inside the network must also be considered. Internal DDoS attacks allow disgruntled or malicious users to disrupt services without any outside influence.

To help protect your network, you can set up filters on external routers to drop packets involved in these types of attacks. You should also set up another filter that denies traffic originating from the Internet that shows an internal network address. When you do this, the loss of ping and some services and utilities for testing network connectivity will be incurred, but this is a small price to pay for network protection. If the operating system allows it, reduce the amount of time before the reset of an unfinished TCP connection. Doing so makes it harder to keep resources unavailable for extended periods of time.

TIP

In the case of a DDoS attack, your best weapon is to get in touch quickly with your upstream Internet service provider (ISP) and see whether it can divert traffic or block the traffic at a higher level.

Subscribing to newsgroups and checking security websites daily ensures that you keep up with the latest attacks and exploits. Applying the manufacturer's latest operating system patches or fixes can also help prevent attacks.

DNS Kiting

A newly registered domain name can be deleted or dropped with full refund of the registration fee during an initial five-day window called the add grace period (AGP). *DNS kiting* refers to the practice of taking advantage of this AGP to monopolize domain names without ever paying for them. How domain kiting works is that a domain name is deleted during the five-day AGP and immediately re-registered for another five-day period. This process is continued constantly, resulting in the domain being registered without actually paying for it.

DNS kiting can be done on a large scale. In this instance, hundreds or thousands of domain names are registered, populated with advertisements, and then canceled just before the five-day grace period. The amount of revenue generated by an individual kited domain is very small. However, there is no cost, and automation allows the registration of multiple domains.

Besides automatically registering domain names and placing advertising, domain kiters can track the amount of revenue generated. This is called domain tasting. It is used to test the profitability of domain names. The AGP is used as a cost-benefit period to determine whether traffic generated by the domain name can offset the registration cost.

EXAM ALERT

Kited domains present several issues. They force search engines to return less-relevant results, tie up domain names that legitimate businesses may want to use, and capitalize on slight variations of personal or business website addresses.

The drawback for domain kiters is the chance that when the domain name is dropped at the end of the AGP, it will not be successfully re-registering.

DNS kiting can be eliminated if registrars such as the Internet Corporation for Assigned Names and Numbers (ICANN) stop the AGP practice, limit how many domains a client can register per day, or refuse to issue repeated refunds to the same client. It has also been suggested that if the ICANN portion of the registration fee were nonrefundable, the practice would stop.

DNS Poisoning

DNS poisoning enables a perpetrator to redirect traffic by changing the IP record for a specific domain, thus permitting the attacker to send legitimate traffic anywhere he chooses. This not only sends a requestor to a different website but also

caches this information for a short period, distributing the attack's effect to the server users. DNS poisoning may also be referred to as DNS cache poisoning because it affects the information that is cached.

All Internet page requests start with a DNS query. If the IP address is not known locally, the request is sent to a DNS server. There are two types of DNS servers: authoritative and recursive. DNS servers share information, but recursive servers maintain information in cache. This means a caching or recursive server can answer queries for resource records even if it can't resolve the request directly. A flaw in the resolution algorithm allows the poisoning of DNS records on a server. All an attacker has to do is delegate a false name to the domain server along with a providing a false address for the server. For example, an attacker creates a hostname hack.hacking.biz. After that, the attacker queries your DNS server to resolve the host hacking.biz. The DNS server resolves the name and stores this information in its cache. Until the zone expiration, any further requests for hacking.biz do not result in lookups but are answered by the server from its cache. It is now possible for me to set your DNS server as the authoritative server for my zone with the domain registrar. If the attacker conducts malicious activity, the attacker can make it appear that your DNS server is being used for these malicious activities.

DNS poisoning can result in many different implications. Domain name servers can be used for DDoS attacks. Malware can be downloaded to an unsuspecting user's computer from the rogue site, and all future requests by that computer will be redirected to the fake IP address. This could be used to build an effective botnet. This method of poisoning could also allow for cross-site scripting exploits, especially because Web 2.0 capabilities allow content to be pulled from multiple websites at the same time.

To minimize the effects of DNS poisoning, check the DNS setup if you are hosting your own DNS. Be sure the DNS server is not open-recursive. An open-recursive DNS server responds any lookup request, without checking where it originates. Disable recursive access for other networks to resolve names that are not in your zone files. You can also use different servers for authoritative and recursive lookups and require that caches discard information except from the com servers and the root servers. From the user perspective, education works best. However, it is becoming more difficult to spot a problem by watching the address bar on the Internet browser. Therefore, operating system vendors are adding more protection. Microsoft Vista's User Account Control (UAC) notifies the user that a program is attempting to change the system's DNS settings, thus preventing the DNS cache from being poisoned.

ARP Poisoning

All network cards have a unique 48-bit address that is hard-coded into the network card. For network communications to occur, this hardware address must be associated with an IP address. Address Resolution Protocol (ARP), which operates at Layer 2 (data link layer) of the Open Systems Interconnect (OSI) model, associates MAC addresses to IP addresses. ARP is a lower-layer protocol that is simple and consists of requests and replies without validation. However, this simplicity also leads to a lack of security.

When you use a protocol analyzer to look at traffic, you see an ARP request and an ARP reply, which are the two basic parts of ARP communication. There are also Reverse ARP (RARP) requests and RARP replies. Devices maintain an ARP table that contains a cache of the IP addresses and MAC addresses the device has already correlated. The host device searches its ARP table to see whether there is a MAC address corresponding to the destination host IP address. When there is no matching entry, it broadcasts an ARP request to the entire network. The broadcast is seen by all systems, but only the device that has the corresponding information relies. However, devices can accept ARP replies before even requesting them. This type of entry is known as an unsolicited entry because the information was not explicitly requested.

EXAM ALERT

Because ARP does not require any type of validation, as ARP requests are sent, the requesting devices believe that the incoming ARP replies are from the correct devices. This can allow a perpetrator to trick a device into thinking any IP is related to any MAC address.

In addition, they can broadcast a fake or spoofed ARP reply to an entire network and poison all computers. This is known as *ARP poisoning*. Put simply, the attacker deceives a device on your network, poisoning its table associations of other devices.

ARP poisoning can lead to attacks such as DoS, man-in-the-middle attacks, and MAC flooding. DoS and man-in-the-middle attacks were discussed earlier in this chapter. MAC flooding is an attack directed at network switches. This type of attack is successful because of the nature of the way all switches and bridges work. The amount of space allocated to store source addresses of packets is very limited. When the table becomes full, the device can no longer learn new information and becomes flooded. As a result, the switch can be forced into a hub-like state that will broadcast all network traffic to every device in the network.

An example of this is a tool called Macof. Macof floods the network with random MAC addresses. Switches may then get stuck in open-repeating mode, leaving the network traffic susceptible to sniffing. Nonintelligent switches do not check the sender's identity, thereby allowing this condition to happen.

A lesser vulnerability of ARP is port stealing. Port stealing is a man-in-the-middle attack that exploits the binding between the port and the MAC address. The principle behind port stealing is that an attacker sends numerous packets with the source IP address of the victim and the destination MAC address of the attacker. This attack applies to broadcast networks built from switches.

ARP traffic operates at Layer 2 (data link layer) of the OSI model and is broadcast on local subnets. ARP poisoning is limited to attacks that are local-based, so an intruder needs either physical access to your network or control of a device on your local network. To mitigate ARP poisoning on a small network, you can use static or script-based mapping for IP addresses and ARP tables. For large networks, use equipment that offers port security. By doing so, you can permit only one MAC address for each physical port on the switch. In addition, you can deploy monitoring tools or an intrusion detection system (IDS) to alert you when suspect activity occurs.

Network Design Elements and Components

As you create a network security policy, you must define procedures to defend your network and users against harm and loss. With this objective in mind, a network design and the included components play an important role in implementing the overall security of the organization.

An overall security solution includes design elements and components such as firewalls, VLANS, and perimeter network boundaries that distinguish between private networks, intranets, and the Internet. This section discusses these elements and will help you tell them apart and understand their function in the security of the network.

Demilitarized Zone

A *demilitarized zone* (DMZ) is a small network between the internal network and the Internet that provides a layer of security and privacy. Both internal and external users may have limited access to the servers in the DMZ. Figure 3.3 depicts a DMZ.

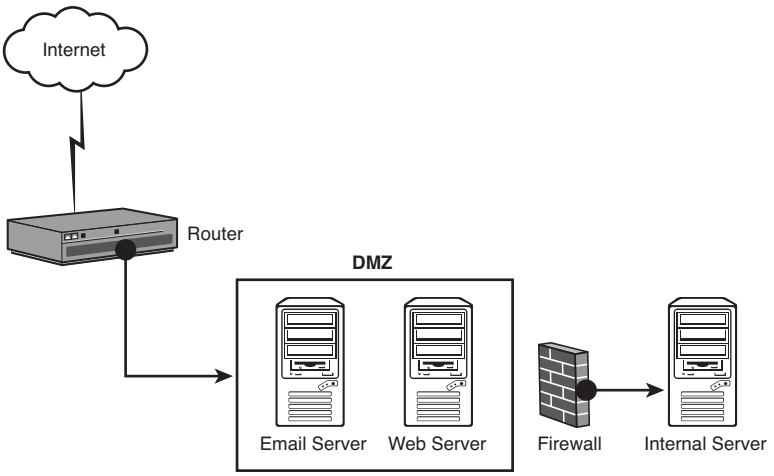

FIGURE 3.3 A DMZ.

Often, web and mail servers are placed in the DMZ. Because these devices are exposed to the Internet, it is important that they are hardened and patches are kept current. Table 3.2 lists the most common services and ports that are run on servers inside the DMZ.

TABLE 3.2 Commonly Used Ports on Servers in the DMZ

Port	Service
21	FTP
22	SSH
25	SMTP
53	DNS
80	HTTP
110	POP3
443	HTTPS

The DMZ is an area that allows external users to access information that the organization deems necessary but will not compromise any internal organizational information. This configuration allows outside access, yet prevents external users from directly accessing a server that holds internal organizational data.

Intranet

An *intranet* is a portion of the internal network that uses web-based technologies. The information is stored on web servers and accessed using browsers. Although web servers are used, they don't necessarily have to be accessible to the outside world. This is possible because the IP addresses of the servers are reserved for private, internal use. You learn more about private IP addresses in the "NAT" section, later in this chapter. If the intranet can be accessed from public networks, it should be through a virtual private network (VPN) for security reasons. VPNs are described in greater detail in Chapter 6, "Securing Communications."

Extranet

An *extranet* is the public portion of the company's IT infrastructure that allows resources to be used by authorized partners and resellers that have proper authorization and authentication. This type of arrangement is commonly used for business-to-business relationships. Because an extranet can provide liability for a company, care must be taken to ensure that VPNs and firewalls are configured properly and that security policies are strictly enforced.

Virtual Local Area Network

The purpose of a *virtual local area network* (VLAN) is to unite network nodes logically into the same broadcast domain regardless of their physical attachment to the network. VLANs provide a way to limit broadcast traffic in a switched network. This creates a boundary and, in essence, creates multiple, isolated LANs on one switch. Because switches operate on Layer 2 (data link layer) of the OSI model, a router is required if data is to be passed from one VLAN to another.

EXAM ALERT

The purpose of a VLAN is to logically group network nodes regardless of their physical location.

Frame tagging is the technology used for VLANs. The 802.1Q standard defines a mechanism that encapsulates the frames with headers, which then tags them with a VLAN ID. VLAN-aware network devices look for these tags in frames and make appropriate forwarding decisions. A VLAN is basically a software

solution that allows creating unique tag identifiers to be assigned to different ports on the switch.

The most notable benefit of using a VLAN is that it can span multiple switches. Because users on the same VLAN don't have to be associated by physical location, they can be grouped by department or function. Here are the benefits that VLANs provide:

- Users can be grouped by department rather than physical location.
- Moving and adding users is simplified. No matter where a user physically moves, changes are made to the software configuration in the switch.
- Because VLANs allow users to be grouped, applying security policies becomes easier.

Keep in mind that use of a VLAN is not an absolute safeguard against security infringements. It does not provide the same level of security as a router. A VLAN is a software solution and cannot take the place of a well subnetted or routed network. It is possible to make frames hop from one VLAN to another. This takes skill and knowledge on the part of an attacker, but it is possible. For more information about frame tagging and VLANs, see the "Suggested Reading and Resources" section at the end of the chapter.

Network Address Translation

Network Address Translation (NAT) acts as a liaison between an internal network and the Internet. It allows multiple computers to connect to the Internet using one IP address. An important security aspect of NAT is that it hides the internal network from the outside world. In this situation, the internal network uses a private IP address. Special ranges in each IP address class are used specifically for private addressing. These addresses are considered nonroutable on the Internet.

Here are the private address ranges:

- *Class A*—10.0.0.0 network. Valid host IDs are from 10.0.0.1 to 10.255.255.254.
- *Class B*—172.16.0.0 through 172.31.0.0 networks. Valid host IDs are from 172.16.0.1 through 172.31.255.254.
- *Class C*—192.168.0.0 network. Valid host IDs are from 192.168.0.1 to 192.168.255.254.

For smaller companies, NAT can be used in the form of Windows Internet Connection Sharing (ICS), where all machines share one Internet connection, such as a dial-up modem. NAT can also be used for address translation between multiple protocols, which improves security and provides for more interoperability in heterogeneous networks.

NOTE

Keep in mind that NAT and IPsec may not work well together. NAT has to replace the headers of the incoming packet with its own headers before sending the packet. This might not be possible because IPsec information is encrypted.

TIP

Another address range to keep in mind when designing IP address space is Automatic Private IP Addressing (APIPA). In the event that no Dynamic Host Configuration Protocol (DHCP) server is available at the time that the client issues a DHCP lease request, the client is automatically configured with an address from the 169.254.0.1 through 169.254.255.254 range.

Subnetting

Subnetting can be done for several reasons. If you have a Class C address and 1,000 clients. you will have to subnet the network or use a custom subnet mask to accommodate all the hosts. The most common reason networks are subnetted is to control network traffic. Splitting one network into two or more and using routers to connect each subnet together means that broadcasts can be limited to each subnet. However, often networks are subnetted to improve network security, not just performance. Subnetting allows you to arrange hosts into the different logical groups that isolate each subnet into its own mini network. Subnet divisions can be based on business goals and security policy objectives. For example, perhaps you use contract workers and want to keep them separated from the organizational employees. Often, organizations with branches use subnets to keep each branch separate. When your computers are on separate physical networks, you can divide your network into subnets that enable you to use one block of addresses on multiple physical networks. If an incident happens and you notice it quickly, you can usually contain the issue to that particular subnet.

IP Classes

In case you are unclear about IP classes, the following information will help you review or learn about the different classes. IP address space is divided into five classes: A, B, C, D, and E. The first byte of the address determines which class an address belongs to:

- Network addresses with the first byte between 1 and 126 are Class A and can have about 17 million hosts each.
- Network addresses with the first byte between 128 and 191 are Class B and can have about 65,000 hosts each.
- Network addresses with the first byte between 192 and 223 are Class C and can have about 250 hosts.
- Network addresses with the first byte between 224 and 239 are Class D and are used for multicasting.
- Network addresses with the first byte between 240 and 255 are Class E and are used as experimental addresses.

Notice that the 127 network address is missing. Although the 127.0.0.0 network is in technically in the Class A area, using addresses in this range causes the protocol software to return data without sending traffic across a network. For example, the address 127.0.0.1 is used for TCP/IP loopback testing, and the address 127.0.0.2 is used by most DNS black lists for testing purposes. Should you need additional review on IP addressing and subnetting, a wide variety of information is available. One such website is Learntosubnet.com. Figure 3.4 shows an internal network with two different subnets. Notice the IP addresses, subnet masks, and default gateway.

EXAM ALERT

Watch for scenarios or examples such as Figure 3.4 asking you to identify a correct/incorrect subnet mask, default gateway address, or router.

IPv6 is designed to replace IPv4. Addresses are 128 bits rather than the 32 bits used in IPv4. Just as in IPv4, blocks of addresses are set aside in IPv6 for private addresses. In IPv6, internal addresses are called unique local addresses (ULA). Addresses starting with fe80: are called link-local addresses and are routable only in the local link area. IPv6 addresses are represented in hexadecimal. For more information about IPv6, visit http://www.ipv6.org/.

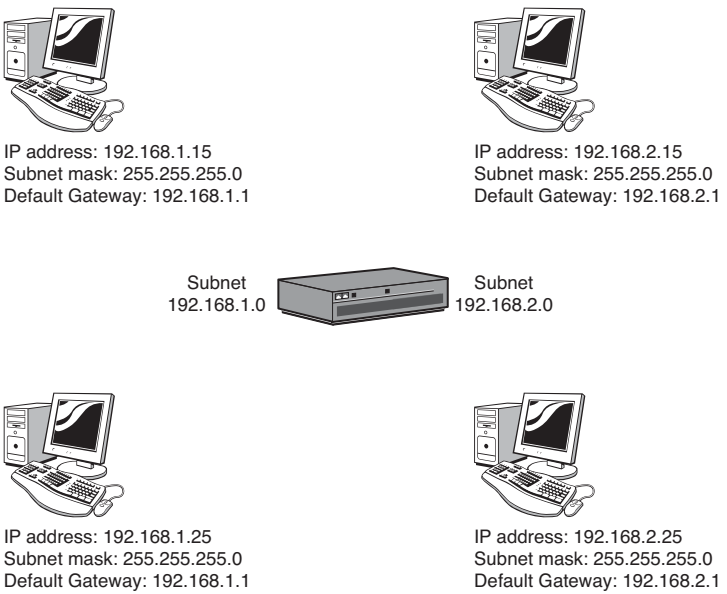

FIGURE 3.4 A segmented network. Notice the subnets 192.168.1.0 and 192.168.2.0 identified next to the router. These are not valid IP addresses for a network router and are used to identify the 192.168.1.x and 192.168.2.x networks in routing tables.

Network Interconnections

Besides securing ports and protocols from outside attacks, connections between interconnecting networks should be secured. This situation may come into play when an organization establishes network interconnections with partners. This might be in the form of an extranet or actual connection between the involved organizations as in a merger, acquisition, or joint project. Business partners can include government agencies and commercial organizations. Although this type of interconnection increases functionality and reduces costs, it can result in security risks. These risks include compromise of all connected systems and any network connected to those systems, along with exposure of data the systems handle. With interconnected networks, the potential for damage greatly increases because one compromised system on one network can easily spread to other networks.

Organizational policies should require an interconnection agreement for any system or network that shares information with another external system or network. Organizations need to carefully evaluate risk-management procedures and ensure that the interconnection is properly designed. The partnering organizations have little to no control over the management of the other party's

system, so without careful planning and assessment, both parties can be harmed. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*, provides guidance for any organization that is considering interconnecting with a government agency or other organization.

Network Access Control

One the most effective ways to protect the network from malicious hosts is to use network access control (NAC). NAC offers a method of enforcement that helps ensure computers are properly configured. The premise behind NAC is to secure the environment by examining the user's machine and based on the results grant (or not grant) access accordingly. It is based on assessment and enforcement. For example, if the user's computer patches are not up-to-date, and no desktop firewall software is installed, you can decide whether to limit access to network resources. Any host machine that doesn't comply with your defined policy could be relegated to remediation server, or put on a guest VLAN. The basic components of NAC products are

- *Access requestor (AR)*—This is the device that requests access. The assessment of the device can be self-performed or delegated to another system.
- *Policy decision point (PDP)*—This is the system that assigns a policy based on the assessment. The PDP determines what access should be granted and may be the NAC's product-management system.
- *Policy enforcement point (PEP)*—This is the device that enforces the policy. This device may be a switch, firewall, or router.

The four ways NAC systems can be integrated into the network are

- *Inline*—An appliance in the line, usually between the access and the distribution switches
- *Out-of-band*—Intervenes and performs an assessment as hosts come online and then grants appropriate access
- *Switch based*—Similar to inline NAC except enforcement occurs on the switch itself
- *Host based*—Relies on an installed host agent to assess and enforce access policy

In addition to providing the ability to enforce security policy, contain noncompliant users, and mitigate threats, NAC offers a number of business benefits.

The business benefits include compliance, a better security posture, and operational cost management.

Telephony

The transmission of data through equipment in a telecommunications environment is known as *telephony*. Telephony includes transmission of voice, fax, or other data. This section describes the components that need to be considered when securing the environment. Often, these components are neglected because they are not really network components. However, they use communications equipment that is susceptible to attack and therefore must be secured.

Telecom/PBX

The telecommunications (telecom) system and Private Branch Exchange (PBX) are a vital part of an organization's infrastructure. Besides the standard block, there are also PBX servers, where the PBX board plugs into the server and is configured through software on the computer. Many companies have moved to Voice over IP (VoIP) to integrate computer telephony, videoconferencing, and document sharing.

For years PBX-type systems have been targeted by hackers, mainly to get free long-distance service. The vulnerabilities that phone networks are subject to include social engineering, long-distance toll fraud, and breach of data privacy.

To protect your network, make sure the PBX is in a secure area, any default passwords have been changed, and only authorized maintenance is done. Many times, hackers can gain access to the phone system via social engineering because this device is usually serviced through a remote maintenance port.

Voice over Internet Protocol

VoIP uses the Internet to transmit voice data. A VoIP system might be composed of many different components, including VoIP phones, desktop systems, PBX servers, and gateways. VoIP PBX servers are susceptible to the same type of exploits as other network servers. These attacks include DoS and buffer overflows, with DoS being the most prevalent. In addition, there are voice-specific attacks and threats. H.323 and Inter Asterisk eXchange (IAX) are specifications and protcols for audio/video. They enable VoIP connections between servers and enable client/server communication. H.323 and IAX protocols can be vulnerable to sniffing during authentication. This allows an attacker to obtain passwords that may be used to compromise the voice network. Session Initiation Protocol (SIP) is commonly used in instant messaging, but it can also be used as an alternative for VoIP. Using SIP can leave VoIP networks open to unauthorized transport of data. Man-in-the-middle attacks between the SIP phone and

SIP proxy allow the audio to be manipulated, causing dropped, rerouted, or playback calls. Many components comprise a VoIP network, and VoIP security is built upon many layers of traditional data security. Therefore, access can be gained in a lot of areas.

Implementing the following solutions can help mitigate the risks and vulnerabilities associated with VoIP:

- Encryption
- Authentication
- Data validation
- Nonrepudiation

Modems

Modems are used via the phone line to dial in to a server or computer. They are gradually being replaced by high-speed cable and Digital Subscriber Line (DSL) solutions, which are faster than dial-up access. However, some companies still use modems for employees to dial into the network and work from home. The modems on network computers or servers are usually configured to take incoming calls. Leaving modems open for incoming calls with little to no authentication for users dialing in can be a clear security vulnerability in the network. For example, war-dialing attacks take advantage of this situation. War-dialing is the process by which an automated software application is used to dial numbers in a given range to determine whether any of the numbers are serviced by modems that accept dial-in requests. This attack can be set to target connected modems that are set to receive calls without any authentication, thus allowing attackers an easy path into the network. You can resolve this problem area in several ways:

- Set the callback features to have the modem call the user back at a preset number.
- Make sure authentication is required using strong passwords.
- Be sure employees have not set up modems at their workstations with remote-control software installed.

Cable and DSL modems are popular these days. They act more like routers than modems. Although these devices are not prone to war-dialing attacks, they do present a certain amount of danger by maintaining an always-on connection. If you leave the connection on all the time, a hacker has ample time to get into the machine and the network. The use of encryption and firewall solutions will help keep the environment safe from attacks.

Network Security Tools

The easiest way to keep a computer safe is by physically isolating it from outside contact. The way most companies do business today makes this virtually impossible. Our networks and environments are becoming increasingly more complex. Securing the devices on the network is imperative to protecting the environment. To secure devices, you must understand the basic security concepts of network security tools. This section introduces security concepts as they apply to the physical security devices used to form the protection found on most networks.

NIDS and HIDS

IDS stands for *intrusion-detection system*. Intrusion-detection systems are designed to analyze data, identify attacks, and respond to the intrusion. They are different from firewalls in that firewalls control the information that gets in and out of the network, whereas IDSs can identify unauthorized activity. IDSs are also designed to catch attacks in progress within the network, not just on the boundary between private and public networks. The two basic types of IDSs are *network-based* and *host-based*. As the names suggest, network-based IDSs (NIDSs) look at the information exchanged between machines, and host-based IDSs (HIDSs) look at information that originates on the individual machines. Here are some basics:

- NIDSs monitor the packet flow and try to locate packets that may have gotten through the firewall and are not allowed for one reason or another. They are best at detecting DoS attacks and unauthorized user access.
- HIDSs monitor communications on a host-by-host basis and try to filter malicious data. These types of IDSs are good at detecting unauthorized file modifications and user activity.

EXAM ALERT

NIDSs try to locate packets not allowed on the network that the firewall missed. HIDSs collect and analyze data that originates on the local machine or a computer hosting a service. NIDSs tend to be more distributed.

NIDSs and HIDSs should be used together to ensure a truly secure environment. IDSs can be located anywhere on the network. They can be placed internally or between firewalls. Many different types of IDSs are available, all with

different capabilities, so make sure they meet the needs of your company before committing to using them. Chapter 7, "Intrusion Detection and Security Baselines," covers IDSs in more detail.

Network Intrusion Prevention System

Network intrusion-prevention systems (NIPSs) are sometimes considered to be an extension of IDSs. NIPSs can be either hardware- or software-based, like many other network-protection devices. Intrusion prevention differs from intrusion detection in that it actually prevents attacks instead of only detecting the occurrence of an attack. Intrusion-detection software is reactive, scanning for configuration weaknesses and detecting attacks after they occur. By the time an alert has been issued, the attack has usually occurred and has damaged the network or desktop. NIPS are designed to sit inline with traffic flows and prevent attacks in real time. An inline NIPS works like a Layer 2 bridge. It sits between the systems that need to be protected and the rest of the network. They proactively protect machines against damage from attacks that signature-based technologies cannot detect because most NIPS solutions can look at application layer protocols such HTTP, FTP, and SMTP.

When implementing a NIPS, keep in mind that the sensors must be physically inline to function properly. This adds single points of failure to the network. A good way to prevent this issue is to use fail-open technology. This means that if the device fails, it doesn't cause a complete network outage; instead, it acts like a patch cable. NIPS are explained in greater detail in Chapter 7, "Intrusion Detection and Security Baselines."

Firewalls

A firewall is a component placed on computers and networks to help eliminate undesired access by the outside world. It can be composed of hardware, software, or a combination of both. A firewall is the first line of defense for the network. How firewalls are configured is important, especially for large companies where a compromised firewall may spell disaster in the form of bad publicity or a lawsuit, not only for the company, but also for the companies it does business with. For smaller companies, a firewall is an excellent investment because most small companies don't have a full-time technology staff, and an intrusion could easily put them out of business. All things considered, a firewall is an important part of your defense, but you should not rely on it exclusively for network protection. Figure 3.5 shows a network with a firewall in place.

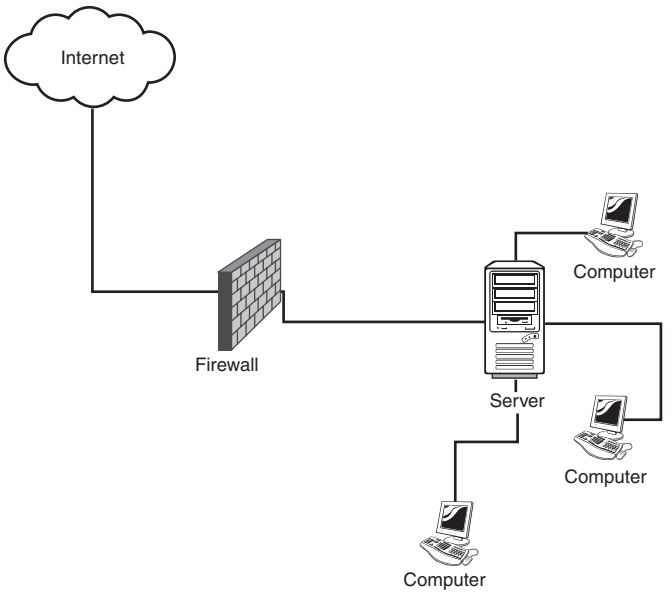

FIGURE 3.5 A network with a firewall.

There are three main types of firewalls:

- Packet-filtering firewall
- Proxy-service firewall, including two types of proxies:
  - Circuit-level gateway
  - Application-level gateway
- Stateful-inspection firewall

The following sections describe each type in detail.

Packet-Filtering Firewall

A packet-filtering firewall is typically a router. Packets can be filtered based on IP addresses, ports, or protocols. They operate at the network layer (Layer 3) of the OSI model. Packet-filtering solutions are generally considered less-secure firewalls because they still allow packets inside the network, regardless of communication pattern within the session. This leaves the system open to DoS attacks. Even though they are the simplest and least secure, they are a good first line of defense. Their main advantage is speed, which is why they are sometimes used before other types of firewalls to perform the first filtering pass.

Proxy Service Firewall

Proxy service firewalls are go-betweens for the network and the Internet. They hide the internal addresses from the outside world and don't allow the computers on the network to directly access the Internet. This type of firewall has a set of rules that the packets must pass to get in or out. It receives all packets and replaces the IP address on the packets going out with its own address and then changes the address of the packets coming in to the destination address. Here are the two basic types of proxies:

- *Circuit-level gateway*—Operates at the OSI session layer (Layer 5) by monitoring the TCP packet flow to determine whether the session requested is a legitimate one. DoS attacks are detected and prevented in circuit-level architecture where a security device discards suspicious requests.
- *Application-level gateway*—All traffic is examined to check for OSI application layer (Layer 7) protocols that are allowed. Examples of this type of traffic are File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Hypertext Transfer Protocol (HTTP). Because the filtering is application-specific, it adds overhead to the transmissions but is more secure than packet filtering.

Stateful-Inspection Firewall

A stateful-inspection firewall is a combination of all types of firewalls. This firewall relies on algorithms to process application layer data. Because it knows the connection status, it can protect against IP spoofing. It has better security controls than packet filtering, but because it has more security controls and features, it increases the attack surface and is more complicated to maintain.

Other Firewall Considerations

In addition to the core firewall components, administrators should consider other elements when designing a firewall solution. These include network, remote-access, and authentication policies. Firewalls can also provide access control, logging, and intrusion notification.

Proxy Servers

A proxy server operates on the same principle as a proxy–level firewall in that it is a go-between for the network and the Internet. Proxy servers are used for

security, logging, and caching. When the proxy server receives a request for an Internet service, it passes through filtering requirements and checks its local cache for previously downloaded web pages. Because web pages are stored locally, response times for web pages are faster, and traffic to the Internet is substantially reduced. The web cache can also be used to block content from websites that you don't want employees to access, such as pornography, social, or peer-to peer networks. This type of server can be used to rearrange web content to work for mobile devices. It also provides better utilization of bandwidth because it stores all your results from requests for a period of time.

TIP

An exposed server that provides public access to a critical service, such as a web or email server, may be configured to isolate it from an organization's network and to report attack attempts to the network administrator. Such an isolated server is referred to as a *bastion host*, named for the isolated towers that were used to provide castles advanced notice of pending assault.

Internet Content Filters

Internet content filters use a collection of terms, words, and phrases that are compared to content from browsers and applications. This type of software can filter content from various types of Internet activity and applications, such as instant messaging, email, and office documents. Content filtering will report only on violations identified in the specified applications listed for the filtering application. In other words, if the application will filter only Microsoft Office documents and a user chooses to use open Office, the content will not be filtered. Internet content filtering works by analyzing data against a database contained in the software. If a match occurs, the data can be addressed in one of several ways, including filtering, capturing, or blocking the content and closing the application. An example of such software is Vista's Parental Controls.

Content filtering requires an agent on each workstation to inspect the content being accessed. If the content data violates the preset policy, a capture of the violating screen is stored on the server with pertinent information relating to the violation. This might include a violation stamp with user, time, date, and application. This information can later be reviewed. Using a predetermined database of specific terminology can help the organization focus on content that violates policy. For example, a sexually explicit database may contain words that are used in the medical industry. Content-filtering applications allow those words that are used in medical context to pass through the filter without reporting a viola-

tion. This same principle enables an organization to monitor for unauthorized transfer of confidential information.

Content filtering is integrated at the operating system level so that it can monitor events such as opening files via Windows Explorer. It can be used to monitor and stop the disclosure of the organization's proprietary or confidential information. Because content filtering uses screen captures of each violation with time-stamped data, it provides proper documentation for forensic investigations and litigation purposes. Unlike antivirus and antispyware applications, content monitoring does not require daily updates to keep the database effective and current. On the downside, content filtering needs to be "trained." For example, to filter nonpornographic material, the terminology must be input and defined in the database.

Protocol Analyzers

Protocol analyzers help you troubleshoot network issues by gathering packet-level information across the network. These applications capture packets and decode the information into readable data for analysis. Protocol analyzers can do more than just look at packets. They prove useful in many other areas of network management, such as monitoring the network for unexpected, unwanted, and unnecessary traffic. For example, if the network is running slowly, a protocol analyzer can tell you whether unnecessary protocols are running on the network. You can also filter specific port numbers and types of traffic so that you can keep an eye on indicators that may cause you problems. Many protocol analyzers can be run on multiple platforms and do live traffic captures and offline analysis. Software USB protocol analyzers are also available for the development of USB devices and analysis of USB traffic.

Exam Prep Questions

1. Your company is in the process of setting up a DMZ segment. You have to allow email traffic in the DMZ segment. Which TCP ports do you have to open? (Choose two correct answers.)

   - ❍ **A.** 110
   - ❍ **B.** 139
   - ❍ **C.** 25
   - ❍ **D.** 443

2. Your company is in the process of setting up a management system on your network, and you want to use SNMP. You have to allow this traffic through the router. Which UDP ports do you have to open? (Choose two correct answers.)

   - ❍ **A.** 161
   - ❍ **B.** 139
   - ❍ **C.** 138
   - ❍ **D.** 162

3. You want to implement a proxy firewall technology that can distinguish between FTP commands. Which of the following types of firewall should you choose?

   - ❍ **A.** Proxy gateway
   - ❍ **B.** Circuit-level gateway
   - ❍ **C.** Application-level gateway
   - ❍ **D.** SOCKS proxy

4. You want to use NAT on your network, and you have received a Class C address from your ISP. What range of addresses should you use on the internal network?

   - ❍ **A.** 10.x.x.x
   - ❍ **B.** 172.16.x.x
   - ❍ **C.** 172.31.x.x
   - ❍ **D.** 192.168.x.x

5. You are setting up a switched network and want to group users by department. Which technology would you implement?

- ❍ **A.** DMZ
- ❍ **B.** VPN
- ❍ **C.** VLAN
- ❍ **D.** NAT

6. You are setting up a web server that needs to be accessed by both the employees and by external customers. What type of architecture should you implement?

- ❍ **A.** VLAN
- ❍ **B.** DMZ
- ❍ **C.** NAT
- ❍ **D.** VPN

7. You have recently had some security breaches in the network. You suspect it may be a small group of employees. You want to implement a solution that will monitor the internal network activity and incoming external traffic. Which of the following devices would you use? (Choose two correct answers.)

- ❍ **A.** A router
- ❍ **B.** A network-based IDS
- ❍ **C.** A firewall
- ❍ **D.** A host-based IDS

8. Services using an interprocess communication share such as network file and print sharing services leave the network susceptible to which of the following attacks?

- ❍ **A.** Spoofing
- ❍ **B.** Null sessions
- ❍ **C.** DNS kiting
- ❍ **D.** ARP poisoning

9. You're the security administrator for a bank. The users are complaining about the network being slow. However, it is not a particularly busy time of the day. You capture network packets and discover that hundreds of ICMP packets have been sent to the host. What type of attack is likely being executed against your network?

   - ❍ **A.** Spoofing
   - ❍ **B.** Man-in-the-middle
   - ❍ **C.** DNS kiting
   - ❍ **D.** Denial of service

10. Your network is under attack. Traffic patterns indicate that an unauthorized service is relaying information to a source outside the network. What type of attack is being executed against you?

   - ❍ **A.** Spoofing
   - ❍ **B.** Man-in-the-middle
   - ❍ **C.** Replay
   - ❍ **D.** Denial of service

Answers to Exam Prep Questions

1. **A, C.** Port 110 is used for POP3 incoming mail, and port 25 is used for SMTP outgoing mail. POP3 delivers mail only, and SMTP transfers mail between servers. Answer B is incorrect because UDP uses port 139 for network sharing. Port 443 is used by HTTPS; therefore, answer D is incorrect.

2. **A, D.** UDP ports 161 and 162 are used by SNMP. Answer B is incorrect because UDP uses port 139 for network sharing. Answer C is incorrect because port 138 is used to allow NetBIOS traffic for name resolution.

3. **C.** An application-level gateway understands services and protocols. Answer A is too generic to be a proper answer. Answer B is incorrect because a circuit-level gateway's decisions are based on source and destination addresses. Answer D is incorrect because SOCKS proxy is an example of a circuit-level gateway.

4. **D.** In A Class C network, valid host IDs are from 192.168.0.1 to 192.168.255.254. Answer A is incorrect because it is a Class A address. Valid host IDs are from 10.0.0.1 to 10.255.255.254. Answers B and C are incorrect because they are both Class B addresses; valid host IDs are from 172.16.0.1 through 172.31.255.254.

5. **C.** The purpose of a VLAN is to unite network nodes logically into the same broadcast domain regardless of their physical attachment to the network. Answer A is incorrect because a DMZ is a small network between the internal network and the Internet that provides a layer of security and privacy. Answer B is incorrect because a virtual private network (VPN) is a network connection that allows you access via a secure tunnel created through an Internet connection. Answer D is incorrect because NAT acts as a liaison between an internal network and the Internet.

6. **B.** A DMZ is a small network between the internal network and the Internet that provides a layer of security and privacy. Answer A is incorrect. The purpose of a VLAN is to unite network nodes logically into the same broadcast domain regardless of their physical attachment to the network. Answer C is incorrect because NAT acts as a liaison between an internal network and the Internet. Answer D is incorrect because a VPN is a network connection that allows you access via a secure tunnel created through an Internet connection.

7. **B, D.** Because you want to monitor both types of traffic, the IDSs should be used together. Network-based intrusion-detection systems monitor the packet flow and try to locate packets that are not allowed for one reason or another and may have gotten through the firewall. Host-based intrusion-detection systems monitor communications on a host-by-host basis and try to filter malicious data. These types of IDSs are good at detecting unauthorized file modifications and user activity. Answer A is incorrect because a router forwards information to its destination on the network or the Internet. A firewall protects computers and networks from undesired access by the outside world; therefore, answer C is incorrect.

8. **B.** A null session is a connection without specifying a user name or password. Null sessions are a possible security risk because the connection is not really authenticated. Answer A is incorrect because spoofing involves modifying the source address of traffic or source of information. Answer C is incorrect because domain kiting refers to the practice of taking advantage of this AGP period to monopolize domain names without even paying for them. Answer D is incorrect because ARP poisoning allows a perpetrator to trick a device into thinking any IP is related to any MAC address.

9. **D.** A ping flood is a DoS attack that attempts to block service or reduce activity on a host by sending ping requests directly to the victim using ICMP. Answer A is incorrect because spoofing involves modifying the source address of traffic or source of information. Answer B is incorrect because a man-in-the middle attack is commonly used to gather information in transit between two hosts. Answer C is incorrect because domain kiting refers to the practice of taking advantage of this AGP period to monopolize domain names without even paying for them.

10. **B.** A man-in-the-middle attack is commonly used to gather information in transit between two hosts. Answer A is incorrect because spoofing involves modifying the source address of traffic or source of information. In a replay, an attacker intercepts traffic between two endpoints and retransmits or replays it later; therefore, answer C is incorrect. Because the purpose of a DoS attack is to deny use of resources or services to legitimate users, answer D is incorrect.

Additional Reading and Resources

1. Davis, David. *What is a VLAN? How to Setup a VLAN on a Cisco Switch*: http://www.petri.co.il/csc_setup_a_vlan_on_a_cisco_switch.htm
2. Grance, Tim, Joan Hash, Steven Peck, Jonathan Smith, and Karen Korow-Diks. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*: http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf
3. Harris, Shon. *CISSP All-in-One Exam Guide*, Fourth Edition. McGraw-Hill Osborne Media, 2007.
4. National Institute of Standards and Technology. *Guidelines on Securing Public Web Servers*, Special Publication 800-44 Version 2: http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf
5. Odom, Wendell. *CCNA Official Exam Certification Library (CCNA Exam 640-802)*, Third Edition. Cisco Press, 2008.
6. Shinder, Thomas W. *The Best Damn Firewall Book Period*, Second Edition. Elsevier, 2007.
7. Simpson, W. RFC 2853, *IP in IP Tunneling*: http://www.ietf.org/rfc/rfc1853

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P – Q

R

S

T

U

V

W

X – Z